No. 17-15611-BB

IN The United States Court of Appeals
For The Eleventh Circuit

United States of America,
Plaintiff-Appellee,

V.

Scott Joseph Trader
Defendant-Appellant.

Memorandum of Law in Support of
Defendants Appeal

Now comes Appellant, Scott Trader, with the instant Memorandum of Law in Support of Defendant's Appeal.

In Support, Appellant Submits the following:

Since Carpenter V. United States, 138 S.Ct. 2206, 201 L.Ed 2d 507 (2018) was decided, a number of federal courts have applied the courts holding in various ways, addressing numerous issues. No issue has been discussed in cases more then IP addresses.

One of the two federal courts of appeals to decide a case Similar to Mr. Trader's is United States V. Contreras, 905 F. 3d 853 (5th Cir. 2018). In Contreras, the defendant used Kik to recieve, distribute, and view child pornography. Although the Same Kik application was used, and Presumably the Same Scope of records from Kik were obtained by the government, Contreras did not challenge the acquisition of the Kik records. Contreras instead challenged the acquisition of Subscriber records from Frontier Communications, the internet Service Provider for his residence. More Specifically, Contreras did not claim his physical movements were tracked, but instead claimed that he had "a reasonable expectation of privacy in the family address" associated with frontiers records.

The Court of Appeals held that there was no

reasonable expectation of privacy in the family address contained within Frontier's records. It's reasoning is simple. "Frontier's records revealed only that the IP address was associated with the Contreras's Brownwood residence. They had no bearing on any person's day-to-day movement." Contreras, 905 F. 3d 853, 857.

The distinguishment here is clear. Mr. Trader is not challenging the records H.S.I. obtained from Comcast, the internet service provider for his residence. If he were, this holding would apply. Instead, Mr. Trader is challenging the acquisition of Kik's records by H.S.I. because they do have a bearing on his day to day movements. Kik's records were generated by use of his cell phone, which "faithfully follows its owner" wherever he goes, not just his residence. These records are a collection of IP addresses, which chronicle more than one IP address (over 40), for more than one time (almost 600 times), over 30 days. The holding in Contreras does not negate Mr. Trader's position, it supports and strengthens it.

Nine District Courts have also attempted to address this issue. All nine are easily distinguished from Mr. Trader's case, or were wrongly decided.

In United States v. Tolbert, 2018 U.S. Dist. Lexis 125944, The District Court addressed the questions of whether Carpenter applys to information gathered by the NCMEC through a cybertip (the cybertip information included one IP address identified as Sending Child Pornography through E-Mail), and whether Carpenter applys to information gathered from a Subpoena Sent to the Internet Service Provider, Centurylink. (As in Contreras, this information only reveals one IP address to one location, Tolberts residence.) Id. at 2018 U.S. Dist Lexis 125944 at 30-34.

The court Concluded Carpenter does not apply to the information gathered in Tolbert because it "is Much more like the bank and telephone records in Smith and Miller than the comprehensive, detailed, and long-term location information in Carpenter." Tolbert, 2018 U.S. Dist. Lexis 125944 at 33. In other words, records of one IP address, revealing one location, one time, does not reveal a

Persons Physical day to day movements. But the 30 days of Kik records generated by Mr. Traders cell phone, did.

Likewise, in United States V. Rosenow, 2018 U.S. Dist. Lexis 198054 (S.D. California, Nov 20, 2018) the District Court addressed whether Carpenter applys to information gathered by the NCMEC as the result of a cybertip (just like in Tolbert, that information reveals only one IP address), and concluded it does not. Rosenow, U.S. Dist. Lexis 198054 at 35-37. The court in Rosenow also discussed whether Carpenter applys to preservation requests issued through 18 U.S.C. 2703(f). Id at 28-33. The court concluded it does not because "The preservation requests in this case did not interfere with the defendants use of his accounts and did not entitle the government to obtain any information without further legal process." Id. at 32 These two issues have no bearing on Mr. Traders case.

However, the district court in Rosenow did conclude that a Subpoena under 2703(d) that was used to obtain IP log-in history and other Data from yahoo and facebook is "Not a Search within

the Meaning of the Fourth amendment". Id. at 32-35
In doing so, the court relied on Smith and Miller, and
the antiquated 9th Cir. case from 2008, United States
V. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).
Forrester Solely addressed the use of a home computer,
which Completely misses the issue of Rosenow's case.
A home computer is not a mobile device, and reveals only
one location's IP address information.

The district court in Rosenow did not address
the tracking of a person's physical Movements through
his cell phone, missing the point of Rosenow's argument.
The court concluded that "The information disclosed
by third partys yahoo and facebook did not reveal
any contents of the account" and therefore "the
defendant had no reasonable expectation of Privacy
in the Subscriber information and the IP log-in
information defendant Voluntarily Provided to the online
Service providers in order to establish and Maintain
his account". Id. at 34. Clearly the district court
did not fully Consider the weight of the Supreme courts
decision in Carpenter which addressed the tracking of
a persons physical Movements, and not the contents

of a persons account. Therefore, Mr. Trader argues that Rosenow was wrongly decided and should not bear on the Merits of Mr. Traders appeal now.

IN United States v. Monroe, 350 F. Supp. 3d 43, 2018 U.S. Dist. Lexis 186998 (D. Rhode Island, Nov. 1, 2018), the court concluded Carpenter does not apply to the IP address information gathered by the use of two 18 U.S.C. 2703(d) orders. The first required a "file Sharing Service to disclose the unique internet Protocol ('IP') address for any device that had downloaded the illicit files" (child pornography), and the second "from the internet Service Provider that disclosed the IP address was assigned to" Monroes residence.

IN So holding, the court in Monroe was not persuaded that the "governments acquisition of a defendants historical cell site location information (C.S.L.I.) from a third party is analogous to the Circumstances here". Id. at Lexis 11, 350 F. Supp. 3d 43, 48-49. More Specifically because only one IP address was disclosed by the file Sharing Service (the one which downloaded pornography), and only one location was disclosed by the Internet Service Provider

(Monroes residence), the disclosures were "not an 'exhaustive chronicle' of his physical or digital activities", and did "not reveal the kind of minutely detailed, historical portrait of 'the whole of a person's physical movements' that concerned the Supreme Court in Carpenter". In its reasoning, the court cited United States v. Tolbert, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018). The records obtained in Monroe, much like the records in Tolbert, are easily distinguished and different in quantity and quality than the records in Mr. Traders case. Mr. Traders K.K records reveal over 40 IP addresses, almost 600 times, for 30 Days, and were generated through the use of a cell phone, not through Mr. Trader's home router connected to his Internet Service Provider.

Just as in Monroe, in United States v. Felton, 2019 U.S. Dist. Lexis 25400 (W.D. Louisiana, Feb. 15, 2019), the court concluded Carpenter did not apply to the Subpoe issued by the government to Comcast Communications for subscriber records which revealed only one IP address, and only one location, Feltons residence. Id. at 4, 13. Felton is distinguished, just as Monroe was, from Mr. Trader, in that Felton did not address the tracking of a persons physical

Movements. The instant case, with Mr. Traders Kik data, does.

IN United States V. PoPa, 2019 U.S. Dist. Lexis 31350 (N.D. Ohio, Feb. 27, 2019) an undercover agent observed a user on a Peer to Peer Network, requesting child pornography. A Subpoena was sent to Time Warner cable, the Internet Service provider for that users IP address, for the Subscriber information regarding that IP address. IN denying PoPa's motion to Suppress, the District court concluded that PoPa "Voluntarily disclosed his Subscriber information to time warner... In doing so, he Surrendered his privacy interest in that information". Id. at 8-10. The court decided the third party doctrine applys to this information, which involves NO day to day tracking of a persons physical movements because only one IP address and one Location were disclosed. Because of the Kik records in Mr. Traders case, the two are distinguished. The Kik records do Show the day to day tracking of a persons physical movements, for 30 days.

Similarly to PoPa, IN United States V. McCutchin, 2019 U.S. Dist Lexis 36811 (D. Arizona, March 7, 2019)

an undercover agent observed that a user accessed child pornography on a Peer-to-Peer file-sharing network. After identifying the internet service provider as Cox Communications, the agent sent Cox a Summons under 19 U.S.C. 1509, requiring that they provide customer/subscriber information relating to the identified IP address. In denying a motion to suppress that information, the district court concluded that "the internet subscriber information differs drastically from the C.S.L.I. obtained in Carpenter. It provides business records that are not detailed or encyclopedic. Subscriber information does not reveal familial, political, professional, religious, sexual associations, or location." Id. at 6

The court decided the third party doctrine applys to this information because there was no tracking of a person's physical movements, which again is the distinguishment between this case and Mr. Traders. The information in McCutchin disclosed one IP address, one time. Mr. Traders Kik data disclosed over 40 different previously unknown IP addresses, almost 600 times, over 30 days. These records are cell phone location records and do reveal the owners physical movements The nature of the records themselves, provide the distinguish

In United States v. Gregory, 2018 U.S. Dist. Lexis 207885 (D. Nebraska, Oct. 29, 2018) The NCMEC recieved a cybertip from Google inc. alleging that a user uploaded an image of child pornography to Google + Photo's. Google sent the user E-mail address and the exact IP address used to upload the image, to the NCMEC. A Subpoena was sent to Cox communications, the internet Service provider associated with the IP address. In denying a motion to Suppress, the district court concluded that the "defendants reliance on carpenter is misplaced. The carpenter decision focused on the comprehensive and detailed information provided by wireless carrier cell site records as to an individuals location history. It did not address whether an Internet Service provider, Such as Cox, could Supply a Subscriber's address in response to an administrative Subpoena or whether an individual Maintains an expectation of privacy when using the internet from his or her own residence."

Further, the court concluded that "here the only information Cox provided in response to the Subpoena was the defendants Subscriber information, which included his name, address, and telephone numbers. The response also included

his payment history and the types of service he has with cox. A residential address, particularly one that has previously been provided to a third-Party, does not reveal information about an individual's habits or Movements." Id. at 4-5. The distinguishment in this case, just as in the cases previously distinguished Supra, is the sheer amount of information revealed to the government in the date. Gregory involves only one IP address, only one location, and only one time. "There is a world of difference between the limited types of personal information addressed in [Gregory] and the exhaustive chronicle of location information" collected in Mr. Traders case.

In United States V. Therrien, 2019 U.S. Dist. Lexis 42248 (D. Vermont; March 13, 2019), The government issued a Subpoena to google for the Subscriber information associated with an E-mail account connected to child pornography. Therrien filed a Motion to Suppress, and although this information is Similar to that of Mr. Trader's because "Google produced Subscriber information, Services utilized by the account, the date the account was created, the date and time of the last login, and the IP addresses associated with the account" for almost 100 days, Id. at 3,

The district court denied the motion.

In doing so, the district court cited United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018), United States v. Tolbert, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018), United States v. Rosenow, 2018 U.S. Dist. Lexis 198054, 2018 WL 6064949 at 11 (S.D. Cal. Nov. 20, 2018), and United States v. Felton, 2019 U.S. Dist. Lexis 25400, 2019 WL 659238 at 5 (W.D. La. Feb. 15, 2019) in concluding that "Law enforcement obtained information that an account holder voluntarily turned over to Google. This information is squarely within the third-Party doctrine and requires a different result than in Carpenter. As a result, Defendant did not possess a reasonable expectation of privacy in the information obtained by law enforcement." Id. at 5-7

As explained supra, The four cases cited by the district court in Therrien, and the information obtained by the government within them, are distinguished from Mr. Traders case. Although the information obtained by the government in Therrien and from Mr. Trader are similar, Therrien was wrongly decided, as it relied on distinguished cases.

In United States V. Hood, 2019 U.S. App. Lexis 9817 (1st cir. April 3, 2019), the data at issue obtained by the government, were records from Kik interactive, and the way they were obtained, was through 18 U.S.C. 2702 (c)(4), Just as in Mr. Traoles's case. And although Hood Made the Same argument Mr. Traoles makes today, the first circuit concluded that carpenter does not apply because of two reason's.

First, the court ruled (in part because Hood did not dispute that he voluntarily disclosed the information to Kik) that "an internet user generates the IP address data that the government acquired from Kik in this case only by making the affirmative decision to access a website or application", Unlike C.S.L.I. Id. Lexis 10. This is incorrect.

While this data does generate from accessing a website or application, that is not Solely how it is generated. If a Kik user has the application on his Smartphone, whenever that

user recieves a new message, the application will send a push notification to the phone, which will notify the user of the message. Even if the application is not open, even if the phone is in the user's pocket or in a different room, the user will be notified of the message. There is no doubt that, for the phone to initially recieve the message, the phone has to connect to the internet. When the phone connects to the internet to recieve the message, this data will be generated, without any affirmative act on the part of the user, just as with C.S.L.I. See: Carpenter, 138 S.Ct. at 2211-12

Second, the first circuit concluded that the "IP address data that the government acquired from Kik does not itself convey any location information. The IP address data is merely a string of numbers associated with a device that had, at one time, accessed a wireless network. By contrast, C.S.L.I. itself reveals -- without any independent investigation -- the (at least approximate) location of the cell phone user who generates that data simply by possessing the phone." Id. Lexis 10-11 (emphasis added)

This is also incorrect.

As United States v. Davis, 785 F.3d 498 (11th Cir. 2015) explained, the wireless carriers records produced "five types of data: (1) telephone numbers of calls made by and to Davis's cell phone; (2) whether the call was outgoing or incoming; (3) the date, time, and duration of the call; (4) the number assigned to the cell tower that wirelessly connected the calls from and to Davis; and (5) the Sector number associated with that tower. For ease of reference, the fourth and fifth items are collectively called 'historical cell tower location information.'" Davis, 785 F.3d at 502-03

The "historical cell tower location information" for "Davis's cell number [] showed] only (1) the number of the cell tower used to rate Davis's call, and (2) the Sector number associated with that tower. Thus, to determine the location of any cell tower used" as explained by the employee of the wireless carrier in Davis, Law enforcement would then have to take the next step of viewing

"the cell tower glossary created and kept by MetroPCS. The MetroPCS glossary listed (1) each of its cell tower numbers, (2) the physical address, including latitude and longitude of that cell tower, and (3) how many sectors are within each cell tower's range."
Davis, 785 F. 3d at 504

As Davis clearly explains, C.S.L.I., just as IP address information, is "Metadata", which by definition means: "Data that provides information about other data" Merriam-Webster's collegiate Dictionary (Eleventh edition, principal copyright 2003, 22nd Printing thomson press, September 2018); "Data that describes and gives information about other data" (oxforddictionaries.com, 2015 oxford university press)

Thus, C.S.L.I. does not itself reveal the location of the phone. Like IP address data, C.S.L.I. "is merely a string of numbers associated with a device that had, at one time, accessed a wireless network." There is further investigating by law enforcement that has to be done before obtaining the location of a cell phone, except IP address data gives an exact location of

a cell phone, where C.S.L.I. gives an approximate one. United States v. Hood has been wrongly decided, and since the First Circuit concluded there was no fourth amendment violation, the court did not reach how the information was gathered (the alleged exigent circumstances).

In United States v. Morel, 2019 U.S. App. Lexis 11457 (1st Cir. April 19, 2019), the First Circuit relied upon Hood, decided 16 days prior, to conclude that Carpenter does not apply to the IP address information in the case. Morel is distinguishable to Mr. Trader's case because it involved IP address information provided to the NCMEC (only one IP address, at only one point in time), and the First Circuit may have contradicted their own holding in Hood, by concluding in Morel that "IP address information of the kind and amount collected here -- gathered from an internet company -- simply does not give rise to the concerns identified in Carpenter." Id. at 2019 U.S. app Lexis 16-17. (emphasis added)

By making this statement, the First Circuit

Seems to acknowledge that there may be circumstances where IP address information may be protected by the fourth amendment under Carpenter, if it is of the kind (that reveals location) and amount (Numerous historical IP address connections) that would chronicle a person's past physical movements over an extended period of time. This would give rise to the concerns that were identified in Carpenter.

In United States v. Jenkins, 2019 U.S. Dist. Lexis 63344 (N.D. Ga, Feb 5, 2019), adopted by: United States v. Jenkins, 2019 U.S. Dist. Lexis 62776 (N.D. Ga, April 11, 2019), the district court denied the defendants Motion to Suppress data obtained from Kik. Accepting the Magistrate Judges recommendation, the district court concluded that "This case does not implicate the sort of location surveillance that concerned the Supreme court in Carpenter." Id. Lexis 12. Coming to this conclusion, the court said Jenkins "has not shown, for example, that this information tracks a person's movement with near 'GPS-level precision' like the C.S.L.I. in Carpenter ... that it tracks a persons movements from a public

thoroughfare 'into private residences, doctor's offices, political headquarters, and other potentially revealing locales . . . that it enables the government to obtain 'near perfect surveillance'". Id. Lexis The key distinguishment between JENKINS and Mr. Trader, is Mr. Trader can and has shown this. See: (Reply brief: 1-8)

The facts between the two cases Present the evidence of this. Kik was not the application used in Mr. Trader's case to commit the initial offense. There was not one time when agents could look at Mr. Trader's Kik data and know he was using Kik at a certain time, and at a certain location, to commit a certain offense. This was not the case in JENKINS. Law Enforcement could because Kik was used to commit the offense, there was no need to track any other movements, the exact time and location was already known.

Just as written in Trader's reply brief, Law enforcement had no choice but to track his movements. Kik was not used in the offense, and only his mother owning the home even ties Mr. Trader to that location.

Law Enforcement tracked the activity on Kik, with a large amount coming from that residence's IP address as opposed to other's, and then tracked his movements to determine when he would be connected to the IP address at that location again.

The district court in Jenkins then cited Pre-Carpenter case Law to describe what an IP address is and does, but failed to make the key distinguishments between those records, made with desktop and laptop computers, and Kik's records, made with a Smartphone, Mr. Trader has. (Reply brief: 12-14)

Finally, the district court cited post Carpenter cases that are distinguished (Supra) from Mr. Trader's because of the amount of data obtained by law enforcement. Id. Lexis 12-13. The district court in Jenkins Missed the point of this distinguishment when it concluded that it's "irrelevant". " In Monroe [350 F. Supp. 3d 43 (D.R.I. 2018)] the defendant objected to the production of his IP address" From an on-line file sharing service. (emphasis added). This information only revealed the one IP address (Monroes residence) that was used

to gain access one time (the exact time illicit files were posted on-line). There is a world of difference between the records in Monroe, and records obtained from Kik. Mr. Trader's Kik records revealed over 40 different IP addresses, almost 600 times, over 30 days. If "IP address information Merely Shows the location at which a device accesses the internet during a Specific Session" Id at Lexis 11, then this amount of data does "reveal the kind of minutely detailed, historical portrait of 'the whole of a person's physical movement' that concerned the Supreme Court in Carpenter." Id. Lexis 13. Jenkins was wrongly decided.

Trader is simply requesting this court to follow the factors relied upon in Carpenter by the Supreme Court, and recognize that location data, no matter the form taken, must be evaluated on a case by case basis. To much weight is currently being given to cases both pre and post Carpenter, which reveal substantially less data about a persons physical movements. Mr. Trader's case requires a different result.

U.S. COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

CERTIFICATE OF SERVICE

United States vs. Scott Trader Appeal No. 17-15611-BB

FRAP 25(b) through (d) (see reverse) requires that at or before the time of filing a paper, a party must serve a copy on the other parties to the appeal or review. In addition, the person who made service must certify that the other parties have been served, indicating the date and manner of service, the names of the persons served, and their addresses. **You may use this form to fulfill this requirement.** ***Please type or print legibly.***

I hereby certify that on (date) July 1, 2019,

a true and correct copy of the foregoing (title of filing) Memorandum of Law,

with first class postage prepaid, has been (check one)

☐ deposited in the U.S. Mail

☑ deposited in the prison's internal mailing system

and properly addressed to the persons whose names and addresses are listed below:

Eleventh Circuit Court of Appeals
56 Forsyth Street, N.W., Atlanta, Georgia, 30303
Fletcher Peacock, Federal Public Defender
109 North 2nd Street, Fort Pierce, FL 34950
Emily M. Smachetti, Chief Appellete Division, U.S. Attorneys offic
99 N.E. 4th Street, Miami, Florida 33132

Scott Trader
Your Name (please print)

Scott Trader
Your Signature

Please complete and attach this form to the original document and to any copies you are filing with the court, and to all copies you are serving on other parties to the appeal.

Exhibit J

Transcript of oral argument, dated 11/19/2020

31 pages

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

CASE NO. 2017-15611

D.C. DOCKET NO. 2:17-CR-14047-DMM-1

UNITED STATES OF AMERICA,

Plaintiff/Appellee,

vs.

SCOTT JOSEPH TRADER,

Defendant/Appellant.
_____/

TRANSCRIPT OF PROCEEDINGS
VIA ZOOM VIDEOCONFERENCE
(TRANSCRIBED FROM ELECTRONIC RECORDING)

This cause came on for Oral Argument before the United States Court of Appeals for the Eleventh Circuit via Zoom Videoconference, on the 19th day of November, 2020.

The appearances at said time and place were as follows:

FOR THE PLAINTIFF/APPELLEE:

UNITED STATES ATTORNEY'S OFFICE
BY: CHRISTINE HERNANDEZ, ESQ.
11200 NW 20th Street
Miami, Florida 33172

FOR THE DEFENDANT/APPELLANT:

FEDERAL PUBLIC DEFENDER'S OFFICE
BY: FLETCHER PEACOCK, ESQ.
150 West Flagler Street - Suite 1700
Miami, Florida 33130

(Whereupon, the following is a transcript of the proceedings had on November 19, 2020; the same being transcribed from electronic recording:)

THE CLERK: Hear Ye, Hear Ye, Hear Ye. United States Court of Appeals for the Eleventh Circuit is now open according to law. God save the United States and this Honorable Court.

CHIEF JUDGE PRYOR: Good morning. We have three appeals to hear this morning.

Counsel, I think you know the drill. We're familiar with your cases, we've read your briefs, the authorities cited in your briefs, and we've looked at at least portions of the record. And in the limited time that is available to you this morning, you should feel free to go straight to the heart of your argument. In the event that you're not able to reach some issue that you've briefed, that doesn't mean that it is in any way forfeited, it will still be under submission.

We will probably have some questions this morning. Be mindful of the clock. If you're answering a question from the Court and the time expires, feel free to finish your answer, but do pay attention to when the clock expires and be mindful of our time.

Our first case this morning is United States versus Trader. Mr. Peacock, will you begin?

MR. PEACOCK: Thank you, Your Honor. If it please the Court, Opposing Counsel. Good morning.

CHIEF JUDGE PRYOR: Good morning.

MR. PEACOCK: My name is Fletcher Peacock, I represent Mr. Trader and I represented him below as well.

In this case, Mr. Trader had a reasonable expectation of privacy in the Kik cellular phone records which the Government obtained from the company Kik. Kik is a cellular phone application which only runs on cellular phones. So all of its records are cellular phone records.

Mr. Trader had a reasonable expectation in the privacy of that location information. And that reasonable expectation has been recognized and validated by the United States Supreme Court in the Carpenter case. More importantly, Mr. Trader had a reasonable expectation in the privacy of his own home which was invaded by the Government's surveillance in this case.

That right, as we -- as we know, was established in the cases of United States versus Caira, and Kyllo versus United States many, many years ago.

This case is a hybrid, if you will, of -- of sorts. Carpenter addresses the cell phone records in the hands of a third-party provider, in this case Kik, and recognizes that there is a reasonable expectation of privacy in those records. But it's a hybrid because it also, and perhaps more importantly, concerns the monitoring of Mr. Trader's activities in his home over a 30-day period through obtaining these records.

CHIEF JUDGE PRYOR: The Supreme Court said in Carpenter that it was not addressing other business records that might incidentally reveal location information. Why -- why aren't the IP addresses and e-mail addresses covered by the ordinary third-party doctrine and by, you know, that -- that very clear expression by the Supreme Court in Carpenter to limit its holding and not reach other business records that only incidentally reveal location information?

It seems to me that both IP addresses and e-mail addresses are much more akin to those kinds of business records than the cell site location records.

MR. PEACOCK: Let me respond in two parts, Your Honor.

The first is the whole gist of getting the records from Kik by law enforcement was to obtain

Mr. Trader's locations and to monitor his locations. IP addresses go directly to a location. In the case of a cell phone, a cell phone either uses a wireless network or it uses a cell tower to communicate with however it's intended.

So first of all, those records are not incidentally linked to location, those records are inherently linked to location. But also just as important, when one reads the Carpenter case carefully, Justice Roberts has a very, I think, important quote in there, where he says at Page 2220 "Virtually any activity on the phone generates CSLI," which is cell site location information, "including incoming calls, texts, or e-mails, and countless other data connections that a phone automatically makes when checking for news, weather or social media updates."

And that is exactly what we are talking about here, Your Honor. We are talking about a strictly cellular phone application which the Court clearly anticipated in Carpenter.

CHIEF JUDGE PRYOR: Yeah, but sometimes cell phones generate location information without any affirmative act on the part of the user; isn't that right?

MR. PEACOCK: It depends on the technology. The technology is very complicated. But a cell phone will switch from tower to tower when it's on a -- when it's moving.

CHIEF JUDGE PRYOR: But the only thing the cell phone user can do is -- is to completely shut down the phone. That's the only way to avoid being tracked by these kinds of networks; isn't that right?

MR. PEACOCK: I mean, in reality there are other ways. I mean, first of all, the person doesn't need to take the phone.

CHIEF JUDGE PRYOR: Well, sure. Okay. I'm -- okay.

MR. PEACOCK: Secondly, we have a whole new generation now of phones which are just what we call pay-per-minute phones which are not trackable to any individual. So -- so in essence there is a whole new cellular technology now which is not trackable --

CHIEF JUDGE PRYOR: Your client would have had to have voluntarily and affirmatively acted to open up an app and log in, which would have then disclosed his Internet protocol address; right?

MR. PEACOCK: Well, that -- no, sir. Kik is a two-way application. So he certainly can -- he certainly can contact the application himself from

his cell phone. But once somebody installs the Kik app, just like any app that you might have on your phone, whether it's -- whether it's Google or whatever it is, that app will also seek to contact you and provide you with information.

The way that -- the way that the system works, these companies are very aggressive about trying to get -- push information to the user as well as receive contact from the user. Many of these applications, the information pushed from the provider is much more voluminous than the -- than the contacts made by the actual user.

JUDGE MARCUS: Well, if Trader did not use the app, there would be no IP address logged, would there?

MR. PEACOCK: If he had not installed the app, there would not be, sir.

JUDGE MARCUS: No, I'm asking if he didn't use it.

MR. PEACOCK: No, there still would be. So for instance, when Mr. Trader would be --

JUDGE MARCUS: Without the app open?

MR. PEACOCK: Yes, the app -- so if I'm on the app and when I --

JUDGE MARCUS: Let's assume it's not open.

MR. PEACOCK: Right. Not -- well, it stays open for practical purposes. So once I install the app on my phone, other people from -- throughout the network, the Kik network can send me messages. Kik will then seek out my phone and they will provide me with that message. And in doing so, they will make a record of that incident.

JUDGE MARCUS: Let me go at the question this way. And just help me understand this.

MR. PEACOCK: Yes, sir.

JUDGE MARCUS: If he didn't actually use the app, go to it, turn it on, would there have been any IP address log?

MR. PEACOCK: One of the problems that we have in this case is we don't have an evidentiary record which would answer your question, Your Honor. And I am certainly not an expert.

JUDGE MARCUS: Right. But is there anything in this record that would suggest that if he didn't use the app in the sense that I'm talking about, turning it on, there would be no IP address log. That would be correct, wouldn't it?

MR. PEACOCK: I -- I can't -- I can't answer -- I would be overstepping my -- my technical expertise if I tried to answer that.

I believe, however, Judge, that if Kik sends you a message, yes, there is a record of that IP address, because the service locates you and then provides you with that message.

JUDGE MARCUS: Let me ask you a slightly different question. In your reply brief, you said that there were 593 log-ins, 413 of them from Mr. Trader's home and 180 while he was outside of his home from his phone's data connection or mobile hotspot. There was no cite for that. Where does that come from?

MR. PEACOCK: Your Honor, that was -- those are facts that was alleged in my motion to suppress. The Court did not grant me an evidentiary hearing. So I don't have -- I was not able to place those documents in evidence.

JUDGE MARCUS: So there was no affidavit or whatnot, declaration that would have contained that information?

MR. PEACOCK: No. Those were strictly allegations that -- I mean, it was provided in discovery, Your Honor. That's where I obtained the information from.

JUDGE HULL: Were the documents attached to your motion to suppress?

MR. PEACOCK: No, ma'am.

JUDGE MARCUS: One of the concerns that the Supreme Court raised in Carpenter was that the information essentially was pervasive where the location data created a map of the individual's entire daily life.

Here that would not be the case, would it? The IP address would only show where the Defendant accessed the Kik application, no more, no less; would that be an accurate statement?

MR. PEACOCK: No, sir. No, sir. Because simply -- and you know, volume is certainly not the question under Carpenter. But however, here we do have a lot of volume. And so for 30 continuing days law enforcement was able to monitor Mr. Trader's activities within his own home. Obviously it would have known that he had a cell phone. Obviously it would have known from the timestamps when he was awake, when he was -- you know, when he was resting, all those things.

And as Justice Scalia said in the Kyllo opinion, "All details inside the home are intimate details and they are not the business of law enforcement or the Government in general."

CHIEF JUDGE PRYOR: Mr. Peacock, you saved

five minutes for rebuttal. Let's hear from Miss Hernandez.

MR. PEACOCK: Thank you, sir.

MS. HERNANDEZ: Good morning, Your Honors. May it please the Court. Christine Hernandez on behalf of the United States.

With regard to the first issue alleged in the appellant's brief, I agree with Your Honors' questioning, that this case differs vastly than the Carpenter case to which the appellant squarely relies on. And this is the reason why that it differs.

First and foremost, the Carpenter court found that the collection of cell site location information was so great and of such a magnitude that it chronicled the detailed movements, as Your Honor stated, of people's past movements and potential future movements in ways that technology had never seen before. And this chronicling of this information was done without any active participation of the person that carried the phone.

As Your Honors probably have near you or beside you, everyone here has a cell phone. There are more cell phones in this country than there are people. Unless someone uses a cell phone with regards to an application or a website, an IP address, as Judge

Marcus noted, would not be generated. This is vastly different than cell site location information. Unless, like Chief Judge Pryor indicated, unless you leave the network, unless you turn off the phone, cell site location information is consistently generated. If the phone is on and someone is receiving a phone call or a text message, whether you pick up that phone call or whether you answer that text message, that -- there is going to be a cell site location information.

The Carpenter court found that because of this passive collection of information, there needed to be some protection and found that the third-party doctrine didn't apply. Whereas in this instance, the third-party doctrine clearly applies to the records obtained by Kik in this instance. Because as Judge Marcus indicated, 594 log-ons. That means that over 590 times the appellant in this case went to the Kik application, opened it up and used it.

Now, counsel indicates that -- or indicates that somehow the Kik application is running on the phone, but that is not -- that defies logic in that if you operate a phone, there are certain buttons that you could push on the phone that allows the application to remain open, allows you to remain on. But again,

it is the affirmative acts of an individual that allows that to happen. And that is what happened in this case. The appellant cannot claim that the information that he turned over to Kik to use this application was somehow not turned over voluntarily. He used his e-mail address. He used a user name. He logged on. So there is information in this record that shows that he voluntarily disclosed this information and this information falls squarely under the third-party doctrine.

It's interesting to note that, you know, counsel relies on Carpenter. And Judge Marcus, as you indicated, cell phones are pervasive in our society. The use of cell phones are pervasive in our society. Again, Your Honors probably have your cell phones right next to y'all. I would venture to guess that neither -- or anyone on this Zoom has the Kik application.

CHIEF JUDGE PRYOR: But it would be true, would it not, that the IP address can be used to derive an individual's location?

MS. HERNANDEZ: Judge, I would dispute that. The 26 pages that were turned over in Docket Entry 10 as part of the standing discovery order essentially provides 26 pages of a string of numbers that in and

of itself provides no information.

Had the Kik records provided location information, then the agents in this case would not have had to have done an IP registry search to find out who was the Internet service provider. They would not have had to serve an emergency disclosure request on Comcast. There was no --

JUDGE MARCUS: You're saying that an IP address cannot be used to derive an individual's location?

MS. HERNANDEZ: Judge, based on the records that we have, those 26 pages do not provide location information unless there are additional steps taken by the parties to obtain that information. There are essentially --

JUDGE MARCUS: What additional steps would have to be taken? The reason I ask the question is I may be operating under a misapprehension, but I thought that the IP address can be used to derive an individual's location. This has nothing to do whether the act is passive or active, but just if indeed it is used, would that not enable the Government to pinpoint a location? Mr. Peacock suggests that in 500 -- almost 600 occasions he used it from his home; therefore, you could derive the information that he was at home at the time, and

that on 183 or so other occasions he used it from different locations and you could zero in on each of those locations as well each time that happened.

Have I misunderstood that?

MS. HERNANDEZ: Judge, no, you did not. In this case, the records that were provided by Kik provided an IP address, which essentially are a string of numbers. After they received those records, the agents, based on those 26 pages, did not know the location of where the Kik application had been accessed. So they had to --

CHIEF JUDGE PRYOR: These records are device specific, right, not location?

MS. HERNANDEZ: (Inaudible.)

CHIEF JUDGE PRYOR: These records are device specific. So the IP address would tell you what address -- what device has accessed the Internet, but would not tell you where that device is?

MS. HERNANDEZ: It would give you -- it would give you the device information and it would give you where, in reference to the IP address, the -- the device accessed the particular website or the application. But --

CHIEF JUDGE PRYOR: I know, but -- but for example, if I'm using my cell phone with the Kik app,

(cont'd)

right, and I'm accessing the Internet, the records would disclose the fact that I have done that with that device; right?

MS. HERNANDEZ: (Inaudible.)

CHIEF JUDGE PRYOR: But it would not tell you whether I was at home or at work or somewhere else when I did it?

MS. HERNANDEZ: Judge, it would give you an IP address, but it won't give you a specific location, address. It will give you a --

CHIEF JUDGE PRYOR: It won't tell you the address -- it won't tell you where the device is physically located, will it?

MS. HERNANDEZ: Yes, Judge, that's correct. That's correct.

JUDGE MARCUS: If I were a law enforcement officer and I had the IP address, I would have to take additional steps to pinpoint the location from whence the application was made; do I have that right?

MS. HERNANDEZ: That's exactly correct.

JUDGE MARCUS: What steps would have to be taken and how easy would that be to do?

MS. HERNANDEZ: Well, the steps that would have to be taken, and in this case the steps that were

taken was there would have to be a search in the IP registry address to see who was the provider for that IP address. Once you've identified the provider, you would have to serve some sort of subpoena. In this instance, it was an emergency disclosure request pursuant to 18 U.S.C. 2702, alleging that there was an immediate danger of physical harm. And that would have to be served on the provider. And only if the provider felt that there was an emergency that existed would then those records be released.

JUDGE MARCUS: So if I were a law enforcement agent, I would have to take two additional steps to find out the location, the physical situs from whence I'm logging on and seeking to use that app; do I have that right?

MS. HERNANDEZ: Yes, Your Honor.

JUDGE MARCUS: Thank you.

MS. HERNANDEZ: In addition --

CHIEF JUDGE PRYOR: It's not -- it's really about the location of the device that you'd have to figure out over and above the IP address?

MS. HERNANDEZ: Correct. There are additional steps, as they -- the steps were taken in this case to identify where the location -- where the device accessed this application, and who in fact was the

individual. Because although you may have an IP address, you don't necessarily know who in fact accessed that website or application.

And I want to note that the Carpenter court found that cell site records didn't require the additional steps. The information contained within cell site location information gave law enforcement all the information that they needed to have to see when the -- where the cell phone was, what tower it was nearest, what address that tower was located. And so that's vastly different than the situation that we have here in that agents needed to take the additional steps to figure out where this IP address was registered to, what information they can glean from that address, and whether or not they can locate the individual who was involved, in this case the appellant, with the conversations with the nine-year-old minor child.

So the reliance on Carpenter is very distinguishable here. And that is why the Government filed its supplemental authority that every case before Carpenter and every case since Carpenter has held that IP address information and subscriber information falls squarely under the third-party doctrine. They have found in instances, whether it

was a computer that generated the IP address, or whether it was a cell phone that generated the IP address, they found that when an individual voluntarily discloses information to a third party, in this case the appellant disclosed certain information in order to use the Kik application, they cannot then claim a Fourth Amendment protection or Fourth Amendment right in that information.

In this case, the appellant made the affirmative and volitional steps to access that application, and in doing so, allowed Kik to chronicle that he logged in over 590 times.

But again, it's worthy to note that these 26 pages that were the basis of the motion to suppress, and some reference was made that the Court did deny the motion to suppress, the hearing in this case, and I would submit to the Court that the facts alleged in Docket Entry 13, which was the Defendant's motion to suppress, basically said that these 26 pages provided log-in information and subscriber information and the Court had no additional details that were alleged in Docket Entry 13 that would dispute what the current status of the law was. And that is that those records fell squarely under the third-party doctrine and that the appellant in this case affirmatively

disclosed this information to Kik.

In addition --

CHIEF JUDGE PRYOR: You know, the e-mail address is even further afield, isn't it?

MS. HERNANDEZ: Excuse me? I'm sorry, Your Honor.

CHIEF JUDGE PRYOR: The e-mail address is even further afield, isn't it?

MS. HERNANDEZ: Yes, Judge, e-mail addresses, the contents of the e-mail addresses obviously are -- you know, there are Fourth Amendment protections that concern the contents of e-mails. But the e-mail address that the appellant in this case provided, he voluntarily disclosed that in order to use the Kik application. This is information that individuals turn over in order to use an application, a website.

And Your Honors have phones. Whenever you sign in to an application or you sign in to a website, there are pop-ups where it says "Do you want push notifications --"

JUDGE HULL: Okay. Explain to us where the law enforcement got the e-mail address. Did they get it from the Kik or what --

MS. HERNANDEZ: Yes, Judge Hull, on -- as part of the discovery that was turned over in Docket

Entry 10, the 26 pages showed the IP address, the e-mail information, the user name, and the name that the appellant went by while using the application.

JUDGE HULL: And you explained how you find out the device that's connected with the IP. How do you find out whose e-mail that is?

MS. HERNANDEZ: Well, the -- in this instance, they did not serve any search warrants on that e-mail address in order to obtain more information. What they did was they did a property records search of the home. After they received the Internet subscriber -- Internet provider information that that IP address was registered to a specific residence, they did a property search on -- on that residence and found that Shelly Trader, the appellant's mother, resided there. They also did a Florida DMV search to find that the appellant had listed that residence as his mailing address.

So with regards to, you know, any furtherance of the e-mail address, the appellant's first name is Scott. His last name is Trader. He used -- once they -- they saw that the e-mail address was STrader@yahoo and they saw that someone by the name of Scott Trader listed his mailing address as that

residence, they essentially started putting the pieces together. But they couldn't do that just by virtue of the 26 pages that were provided by Kik. There was an investigation --

CHIEF JUDGE PRYOR: Isn't the answer, though, about the e-mail address that when Trader -- when he registered with Kik to use their app, he voluntarily disclosed an e-mail address to them so that when they then obtained records -- so when -- when the Government obtained records from Kik, that's how they had that e-mail address; isn't that right?

MS. HERNANDEZ: Yes, Chief Judge, that's exactly right. And our common sense tells us every time we go to a website or any time we sign up for an application, the first thing that they ask us is "Input your e-mail address," you know, and they do so for commercial reasons, they do so to be able to contact you. And you can choose whether or not to turn over that information and not use --

CHIEF JUDGE PRYOR: IP addresses are associated with all kinds of devices; right? So there could be household appliances, gaming consoles, any number of devices; isn't that right?

MS. HERNANDEZ: Yes, Judge, they work in conjunction with the Internet provider. And so if

someone uses a gaming console or if someone uses Alexa, for instance, it's going to generate an IP address, but only does so upon the affirmative use of the individual.

CHIEF JUDGE PRYOR: Your time has expired, Miss Hernandez. Do you have anything else to add?

MS. HERNANDEZ: I just wanted to say that we may wake up one day and find that the use of a social media application is as pervasive as a cell phone, but today is not that day and this record before this Court shouldn't extend the Carpenter requirement to issues such as IP addresses.

I will rely on the arguments I made today, as well as those made in the brief, and I thank you for your time.

CHIEF JUDGE PRYOR: Thank you, Miss Hernandez.

Mr. Peacock, you've saved some time for rebuttal.

Mr. Peacock, you need to remove your mute.

MR. PEACOCK: My apologies, Your Honor.

CHIEF JUDGE PRYOR: That's okay.

MR. PEACOCK: The Government's argument focuses on a difference in form, but no difference in substance.

The IP address here is -- is totally about

location, Your Honor. This is what law enforcement does on a regular basis in such cases when they're dealing with Internet-based offenses. They obtain the IP address from whatever medium it is that's being used, they then go to the service provider, which in this case was Comcast. They asked the service provider what -- who the subscriber was for the --

CHIEF JUDGE PRYOR: And that tells you -- that tells you what device is accessing the Internet, but it does not tell you where the device is located or where the user is located. It only tells you -- it only tells you where -- it only tells you what device accessed the Internet.

MR. PEACOCK: No, sir, actually I don't -- I respectfully disagree. In this case in particular, Mr. Trader accessed the wireless Internet system at his mother's house. That wireless Internet router gets an IP number. That's the IP number that they got in this case.

CHIEF JUDGE PRYOR: Uh-huh.

MR. PEACOCK: Any device that hooks up to that wireless system gets what's called a private IP number, which is not published to the outside world. It's only so that that router can recognize

authorized devices on that wireless system at his mother's house.

CHIEF JUDGE PRYOR: You could move the router. It happens to be at her house, but you could move it somewhere else.

MR. PEACOCK: You could --

CHIEF JUDGE PRYOR: And they tell you that.

MR. PEACOCK: Yes, sir, you can move any router, but in this case --

CHIEF JUDGE PRYOR: You can move any device anywhere and it won't tell you -- it just happens to be at her house and -- and you can surmise that it's probably being used there, but in fact you could actually locate it somewhere else.

MR. PEACOCK: Well --

CHIEF JUDGE PRYOR: And the record wouldn't tell you that.

MR. PEACOCK: But Your Honor, if you did that, you would likely get a new IP address. IP addresses contain within that series of numbers geographical information. And that's how those IP addresses are assigned. And so if you -- so you took your router and you moved to California, you would very likely get a new IP address. Now, once again --

CHIEF JUDGE PRYOR: What if you just moved

across town?

MR. PEACOCK: Judge, I don't know. I apologize, I'm not -- I'm not that well-versed on it. But -- and in this case in particular now --

CHIEF JUDGE PRYOR: But my point is this. It does not track your physical movements to the detail that the cell site location records do that were at issue in Carpenter.

MR. PEACOCK: Oh, I believe it's greater than that, Your Honor. I believe it's greater. Because in this case, the agents were able to state to the Court that they had 30 days of monitoring the same IP address at the same physical address. And so they did -- they did use it for monitoring physical location. There's no way to get around that.

JUDGE HULL: Yeah, but in the physical location, those 30 days did not change. It was the home; right?

MR. PEACOCK: Yes, ma'am.

JUDGE HULL: All right. So help me with this. You know, one thing about Carpenter was a telephone. You know, we did toll records forever. We still do toll records. Nobody complains about toll records from phones, a landline phone and you have toll records. You can get toll records, you know that the

toll -- it's tied -- that landline phone is tied to a house. And every time it's used, you know somebody is using it from that one location.

It seems the difference to me is it's this one location. I mean what -- your case is bound up in the facts and one location here. It's not tracking the person. When it's just one location, it's a fixed location. In fact, you just made the point, the router is tied to this location, it's right to -- the device is tied to the router, the router is in the home. We know 30 days it's the home. That seems different than moving -- wherever that guy went, you know, Carpenter -- these cases are robberies, they're moving over to Wendy's, they're going to pizza, they're going around here. We know wherever they went all around town. So that to me is materially different.

Help me with that.

MR. PEACOCK: Yes, ma'am. Well, first off, we need to recognize that approximately 180 of the contacts were with Mobile LTE. Mobile LTE is when a cell phone uses a cell tower. Exactly like what happened in Carpenter. So --

JUDGE HULL: Okay. Was that from different locations or was that from the home location?

MR. PEACOCK: That was from different locations. When the phone leaves the home, it goes off the wireless system --

JUDGE HULL: No, I'm talking about in your case with his IP.

MR. PEACOCK: Yes, ma'am.

JUDGE HULL: Okay.

MR. PEACOCK: Yes, ma'am.

JUDGE HULL: So he took his phone, it's a cell phone application.

MR. PEACOCK: Yes, ma'am. When it gets out of range of the -- of the wireless network at his mother's house, it transfers over to cell site data, which is called Mobile LTE.

JUDGE HULL: And did they -- did they obtain that data? Did they ever get that data?

MR. PEACOCK: They obtained the IP addresses for that --

JUDGE HULL: No, but did they get the data from Mobile LTE about where the cell phone had moved around? If it used cell towers, then whoever -- is Mobile LTE a third party?

MR. PEACOCK: No, Mobile LTE is a technology.

JUDGE HULL: Okay. But did they get --

MR. PEACOCK: No, ma'am.

JUDGE HULL: -- where --

MR. PEACOCK: No, ma'am.

JUDGE HULL: Did they get information where he was when he used Mobile LTE?

MR. PEACOCK: No, ma'am.

JUDGE HULL: Okay.

MR. PEACOCK: They did get the IP addresses for the Mobile LTE, but they did not get cell site information.

JUDGE HULL: Okay. That's --

CHIEF JUDGE PRYOR: Okay. Mr. Peacock, you need to wrap it up, you're a minute over.

MR. PEACOCK: I -- I think I've made my point, Your Honor. I think this was a violation of -- that Carpenter shows there was a reasonable expectation of privacy here.

And then it's not even the diminished expectation in Carpenter, but because it was in the home, it was a full expectation of privacy which the Government violated.

Thank you so much. I'll rely on my briefs for the other arguments in this case.

CHIEF JUDGE PRYOR: Thank you, Mr. Peacock.

MR. PEACOCK: Thank you, Judge.

CHIEF JUDGE PRYOR: We'll move now to our next

case.

(PROCEEDINGS CONCLUDED)

****

STATE OF FLORIDA)

COUNTY OF MARTIN)

CERTIFICATE

I, KATHY CABRE ENLOE, a Registered Professional Reporter, certify that in the matter of UNITED STATES VS. SCOTT TRADER, CASE NO. 17-15611, a hearing was held on November 19, 2020; that the same was electronically recorded, and said recording transcribed by the undersigned. I further certify that the foregoing constitutes a true transcript of the electronically-recorded hearing to the best of my abilities, recognizing those limitations inherent in electronically-recorded proceedings.

I CERTIFY FURTHER that I am neither attorney nor counsel for, nor related to nor employed by any of the parties to the action in which the hearing was had and, further, that I am not a relative or an employee of any attorney or counsel employed in this case; nor am I financially interested in the outcome of this action.

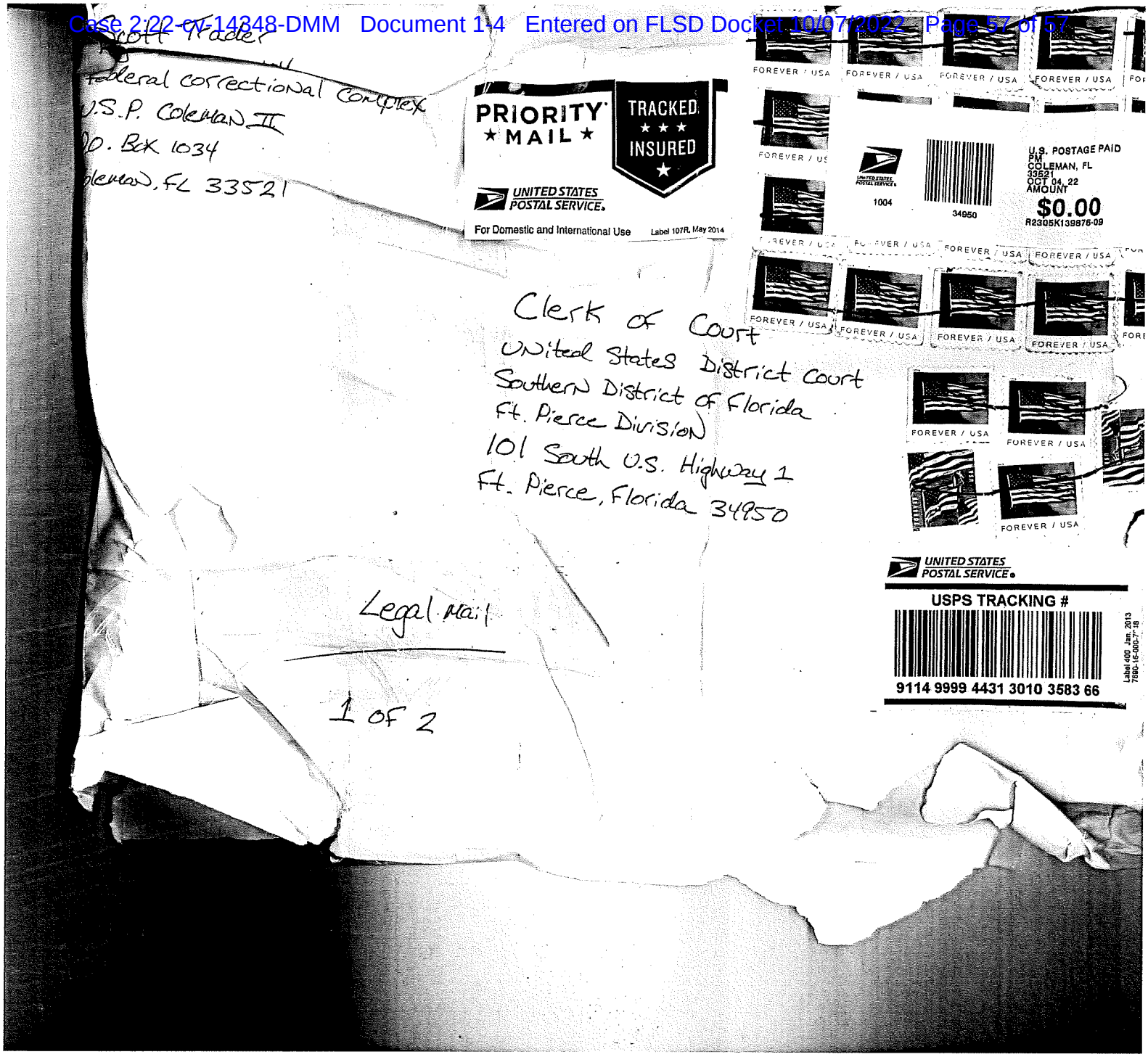
DATED this 8th day of April, 2022

KATHY CABRE ENLOE

Certificate of Service

I HEREBY certify that on this 27 day of September, 2022, I mailed through the prison legal mail system, 1 copys of the foregoing document for delivery to all counsel of record.

/s/ Scott Trader
Scott Trader



Scott Trader
Federal Correctional Complex
U.S.P. Coleman II
P.O. Box 1034
Coleman, FL 33521

PRIORITY MAIL
TRACKED
INSURED
UNITED STATES POSTAL SERVICE.
For Domestic and International Use
Label 107R, May 2014

FOREVER / USA

U.S. POSTAGE PAID
PM
COLEMAN, FL
33521
OCT 04 22
AMOUNT
$0.00
R2305K139876-09

1004
34950

Clerk of Court
United States District Court
Southern District of Florida
Ft. Pierce Division
101 South U.S. Highway 1
Ft. Pierce, Florida 34950

UNITED STATES POSTAL SERVICE.
USPS TRACKING #
9114 9999 4431 3010 3583 66
Label 400 Jan. 2013
7690-16-000-7718

Legal Mail

1 of 2